REMARKS

The Examiner has rejected Claims 1-4, 6-13, 15-22, 24-29 under 35 U.S.C. 102(e) as being unpatentable over Schertz et al. (U.S. Publication No. 2003/0084322 A1) in view of Brook et al. (U.S. Patent No. 7.036,148 B2). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claims 28 and 29.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that "[i]t would have been obvious to...employ the teachings of Brook et al. within the system of Schertz because they are analogous in intrusion detection" and that "[o]ne would have been motivated to incorporate the teachings of Brook et al. because it would provide an efficient detection of intrusion by setting rules like frequency-of-occurrence stipulations, and count-reset instructions with a signature." To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Schertz and Brook references, especially in view of the vast evidence to the contrary.

For example, applicant respectfully notes that the Examiner has failed to cite specific motivation in the above references to support the Examiner's argument that "[o]ne would have been motivated to incorporate the teachings of Brook et al. because it would provide an efficient detection of intrusion by setting rules like frequency-of-occurrence stipulations, and count-reset instructions with a signature." The Examiner is reminded that the Federal Circuit requires that there must be some logical reason apparent from the evidence of record that would justify the combination or modification of references. *In re Regel, 188 USPQ 132 (CCPA 1975).*

In addition, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

In fact, applicant respectfully points out that Schertz only generally discloses "databases 80a and 81a containing known attack signatures" (Paragraph [0021]), and that "[i]f there is match [between a packet and known intrusion signatures and viruses], then remedial or responsive action is taken, such as reporting to the system administrator" (Paragraph [0030]). Clearly, only generally disclosing the use of known intrusion signatures, as in Schertz, fails to provide any suggestion or motivation to specifically utilize business rules that prescribe alterations to intrusion signatures, as in Brook (see Abstract of Brook).

Thus, the first element of the *prima facie* case of obviousness has not been met, for at least the reasons noted above. More importantly, applicant also respectfully asserts that third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts relied upon by the Examiner fail to teach or suggest all of applicant's claim language.

For example, with respect to the independent claims, the Examiner has relied on Paragraphs [0021], [0023], [0018], [0003], and [0030] from Schertz, along with Col. 2, lines 21-55, Col. 4, line 7-Col. 5, line 36 and Col, 3, lines 12-30 from Brook to make a prior art showing of applicant's claimed "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (see this or similar, but not necessarily identical language in each of the independent claims).

First, applicant respectfully asserts that excerpts from Schertz relied on by the Examiner merely teach "monitoring of attempted attacks...and...recording successful attacks" (Paragraph [0021]), and "monitor[ing] all network activity and network traffic" (Paragraph [0003]). In addition, such excerpts teach that "network intrusion protection devices 80 and 81 may be configured...to monitor one or more specific devices rather than all devices on a network" (Paragraph [0023]), and may "analyze data inbound from the Internet and [collect] network packets to compare against a database of various known attack signatures or bit patterns" (Paragraph [0018]). Further, the excerpts teach that "the packet in the frame is compared to known intrusion signatures" (Paragraph [0030]).

Clearly, Schertz only generally discloses monitoring network activity and network traffic for attacks associated with all devices or one or more specific devices on a network, as noted in the excerpts above. Applicant respectfully asserts that simply disclosing such monitoring, as in Schertz, does not specifically teach or suggest "detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added), as applicant claims.

Second, applicant respectfully asserts that excerpts from Brook relied on by the Examiner merely teach that an "intrusion set is altered," and that as an example such

altering includes "set[ting] the logon-password-failure threshold to ten occurrences in twenty minutes" (Col. 2, lines 18-55). In addition, such excerpts teach that "[m]essages flow to the protected network attachment…[which] may constitute an attempt to intrude upon the protected network attachment" (Col. 3, lines 16-22), that individual intrusion sets may include set identifiers, signatures, thresholds, weights, and that individual rules may include rule identifiers, validity conditions, and provisions (Col. 4, line 7-Col. 5, line 36).

Thus, the excerpts from Brook relied on by the Examiner only generally disclose individual intrusion sets that may include thresholds. However, applicant respectfully points out that simply nowhere in such excerpts does Brook specifically disclose "a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added), as applicant claims.

Again, applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since there is not suggestion or motivation to combine the prior art references, and since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 28 and 29 into each of the independent claims.

With respect to the subject matter of former dependent Claim 28 (at least substantially incorporated into each of the independent claims), the Examiner has relied on Paragraph [0021], lines 15-18 in Schertz to make a prior art showing of applicant's claimed technique "wherein predefined network-wide thresholds and patterns are provided as templates."

Applicant respectfully asserts that the excerpt relied on by the Examiner simply discloses that "Network intrusion protection devices 80 and 81 may respectively include

(or alternately be connected to) databases 80a and 81a containing known attack signatures." Clearly, only generally teaching a database containing known attack signatures, as in Schertz, does not even suggest any sort of templates, let alone a specific technique "wherein predefined network-wide thresholds and patterns are provided as templates" (emphasis added), as claimed.

In addition, with respect to the subject matter of former dependent Claim 28 (at least substantially incorporated into each of the independent claims), the Examiner has relied on Paragraph [0021] in Schertz to make a prior art showing of applicant's claimed technique "wherein predefined network-wide thresholds and patterns are customized to particular circumstances."

Applicant again respectfully asserts that the excerpt relied on by the Examiner simply discloses that "[n]etwork intrusion protection devices 80 and 81 may respectively include (or alternately be connected to) databases 80a and 81a containing known attack signatures." Only generally teaching a database containing known attack signatures, as in Schertz, simply does not disclose predefined network-wide thresholds, let alone where such "predefined network-wide thresholds and patterns are customized to particular circumstances" (emphasis added), as specifically claimed.

Since at least the first and third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested. Thus, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the Examiner has rejected Claims 1-4, 6-13, 15-22 and 24-29 under 35 U.S.C. 102(e) as being anticipated by Chefalas et al. (U.S. Patent Publication No. 2002/0116639 A1). Applicant again respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Applicant again points out that applicant has amended the

independent claims to at least substantially include the subject matter of former dependent Claims 28 and 29.

With respect to the independent claims, the Examiner has relied on Paragraph [0012], along with Figures 4A-B and 5A-B from Chefalas to make a prior art showing of applicant's claimed "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (see this or similar, but not necessarily identical language in each of the independent claims). Specifically, applicant notes that the Examiner has argued that such excerpt teaches "multiple patterns are detected and transmitted to the server network-wide threshold."

Applicant respectfully disagrees and asserts that the excerpt from Chefalas relied on by the Examiner merely discloses "automatic detection, notification and elimination of viruses for a large network of machines" and "send[ing] notification of a presence of the virus." However, simply nowhere in such excerpt is there any disclosure of any sort of network-wide threshold, and especially not specifically "a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added), as applicant claims. In addition, the figures relied on by the Examiner only show business events (Figures 4A-B) and policies for taking action in response to notification of a virus (Figures 5A-B). Again, simply nowhere in such Figures is there any disclosure of a network-wide threshold, and especially not in the context claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be

arranged as required by the claim. This criterion has simply not been met by the Chefalas reference, especially in view of the amendments made hereinabove.

The Examiner goes on to admit that the Chefalas reference fails to meet all of applicant's claim language, and then relies on Brook to meet such deficiencies. First, applicant respectfully disagrees with the use of multiple references in such rejection under 35 U.S.C. 102(e), and assumes that the Examiner intended to reject the claims under 35 U.S.C. 103(a) in view of Chefalas and Brook. To this end, applicant incorporates the *obviousness-related* arguments made hereinabove, as well as points out the deficiencies in the reliance on the Brook reference set forth below.

Specifically, with respect to the subject matter of former dependent Claim 28 (at least substantially incorporated into each of the independent claims), the Examiner has relied on items 301B-304B and 301D-304D in Figure 3 of Brook (U.S. Patent No. 7,036,148) to make a prior art showing of applicant's claimed technique "wherein predefined network-wide thresholds and patterns are provided as templates." In response, applicant respectfully asserts that Figure 3 in Brook, as relied on by the Examiner, fails to meet applicant's specific claim language. In particular, items 301B-304B and 301D-304D only show signatures and actions associated with intrusion sets. Simply nowhere in Figure 3, or in the description thereof, is there any disclosure of "predefined network-wide thresholds and patterns [that] are provided as templates" (emphasis added), as applicant specifically claims.

Further, with respect to the subject matter of former dependent Claim 29 (at least substantially incorporated into each of the independent claims), the Examiner has relied on Col. 4, line 7-Col. 5, line 58 from Brook to make a prior art showing of applicant's claimed technique "wherein predefined network-wide thresholds and patterns are customized to particular circumstances." In response, applicant respectfully asserts that the excerpt from Brook, as relied on by the Examiner, fails to meet applicant's specific claim language. For example, the only suggestion of a threshold in Brook relates to individual intrusion sets that may include thresholds, where such thresholds may include

"decision-level information, frequency-of-occurrence stipulations, and count-reset instructions associated with a signature" (Col. 4, lines 22-33). Clearly, such general description of thresholds, as in Brook, fails to specifically teach that "predefined network-wide thresholds and patterns are customized to particular circumstances" (emphasis added), as applicant claims.

Thus, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 6 et al., the Examiner has relied on the following excerpts from Schertz to make a prior art showing of applicant's claimed technique "wherein said at least one predetermined anti-malware action includes isolating at least one of said network connected computers from other parts of said computer network."

> "**Furthermore, OS-integrated anti-virus system 16 would prevent storage of the virus payload (154), and further transmission of the virus payload to other host processors (156).** Finally, execution of the virus payload is also monitored and avoided by OS-integrated anti-virus system 16 (158). These functional blocks may represent either hardware modules or software processes that serve the functionality described." (Paragraph 0031, lines 17-24 - emphasis added)

> "Additionally, an **attack may be prevented because an inline intrusion protection system may discard data identified as associated with an attack** rather than pass the data to the application layer for processing." (Paragraph 0020, lines 14-17 - emphasis added)

Applicant respectfully asserts that the above excerpts from Schertz, as relied upon by the Examiner, simply teach preventing the storage of a virus payload by the anti-virus system and transmission to other host processors. The second excerpt teaches an inline intrusion protection system that may discard data identified as being associated with an attack. The Schertz excerpts, however, fail to even suggest "isolating at least one of said

network connected computers from other parts of said computer network" (emphasis added), as claimed.

In addition, with respect to Claim 7 et al., the Examiner has relied on the following excerpts from Schertz to make a prior art showing of applicant's claimed technique "wherein said managing computer stores said plurality of log data messages within a database."

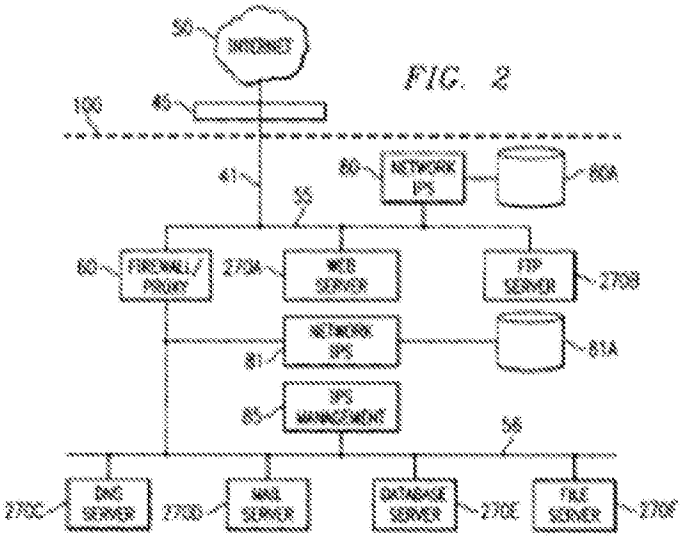

FIG. 2

(Figure 2, items 80A and 81A)

"Network intrusion protection devices 80 and 81 may respectively include (or alternatively be connected to) **databases 80a and 81a containing known attack signatures.**" (Paragraph 0021, lines 15-18 - emphasis added)

Applicant respectfully asserts that items 80A, and 81A in Figure 2 relied upon by the Examiner simply disclose storing known attack signatures in databases for the network intrusion protection devices. Simply storing known attack signatures, as in Schertz, fails to meet applicant claimed technique "wherein said managing computer stores said plurality of log data messages within a database" (emphasis added), as claimed.

Furthermore, with respect to Claim 5 et al., the Examiner has rejected the same as being unpatentable over Schertz, in view of Brook, and in further view of Chen et al (U.S. Patent No. 5,832,208). Specifically, the Examiner has relied on the following

excerpts from Chen to make a prior art showing of applicant's claimed technique "wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning." To provide additional context to item 260 in Figure 3, applicant has included an additional excerpt from Chen below.

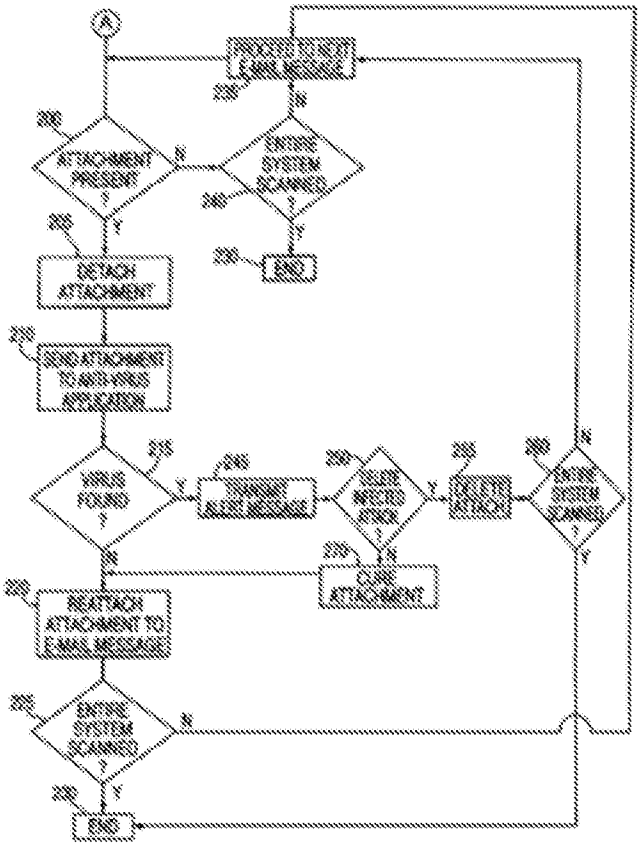

FIG. 3

(Figure 3, item 260)

"After step 255, **the agent 110 determines if the entire mail system 140 has been scanned (step 260).** If so, then the process has reached an end (step 230). If the entire mail system 140 has not been scanned, then the agent 110 proceeds to the next e-mail message (step 235)." (Col. 9, lines 1-5 - emphasis added)

Applicant respectfully asserts that the above figure from Chen relied upon by the Examiner simply teaches scanning an entire mail system, one email message at a time. After processing and handling a virus found in a single email message, the system then

checks to see if the entire mail system was scanned before branching to an end block. Furthermore, if the email attachment does not contain a virus, the system will still check to see if the entire mail system was scanned. Hence, there is no increase in scanning thoroughness after the virus is detected.

This technique of checking all email messages does not even suggest applicant's claimed technique "wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning" (emphasis added), as claimed. Since the Chen excerpts above do not disclose "perform[ing] more thorough malware scanning" (emphasis added), as claimed, such excerpts fail to disclose applicant's claimed technique.

Again, since the prior art excerpts relied on by the Examiner, when taken alone and in combination, fail to teach or suggest all of applicant's specific claim language, as noted above, a notice of allowance or a proper prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 30-34 below, which are added for full consideration:

> "wherein said at least one predetermined anti-malware action is targeted to a particular threat so as to reduce network traffic" (see Claim 30);
>
> "wherein a plurality of said network connected computers associated with said detections utilize outdated malware definition data" (see Claim 31);
>
> "wherein said at least one predetermined anti-malware action includes updating only said network connected computers that utilize said outdated malware definition data" (see Claim 32);

"wherein a plurality of said network connected computers associated with said detections are connected to a particular server" (see Claim 33); and

"wherein said at least one predetermined anti-malware action includes isolating only said particular server and said network connected computers connected thereto" (see Claim 34).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P461).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100